RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: GRC-T09

Using the NIST CSF Maturity Toolkit to Evaluate Your Security Program

John Masserini

Managing Partner
SentiCon Security

https://www.linkedin.com/in/jjmasserini/

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

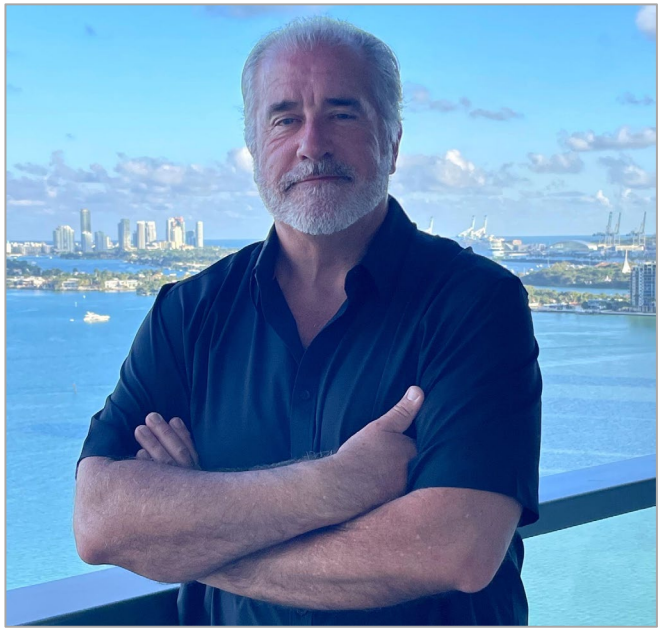
SentiCon Disclaimer: The *NIST CSF Maturity Toolkit* is licensed under the: Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License and is provided "as is," without any warranties or guarantees of any kind, express or implied, including but not limited to warranties of merchantability, fitness for a particular purpose, and non-infringement. The developers and contributors shall not be liable for any claims, damages, or other liabilities arising from the use, misuse, or inability to use this software. Users assume all risks associated with its use and are responsible for compliance with any applicable laws and regulations.

SENTICON SECURITY

John J. Masserini

Founder & Managing Partner, SentiCon Security

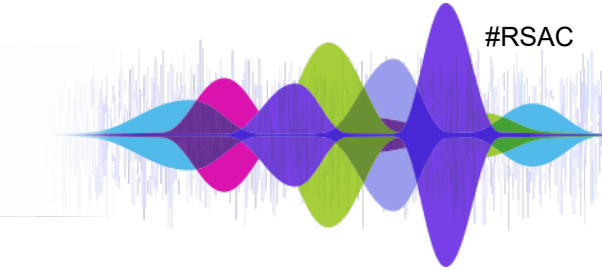
- 30 year cybersecurity veteran
- 3-time, 18-year CISO / Publishing, Finance, Telecommunications
- Publisher of award-winning security blog, ***Chronicles of a CISO***
- Developer of open source ***NIST CSF Maturity Toolkit***, with over 30,000 downloads



RSAC | 2025 Conference

What is the NIST CSF Maturity Toolkit?

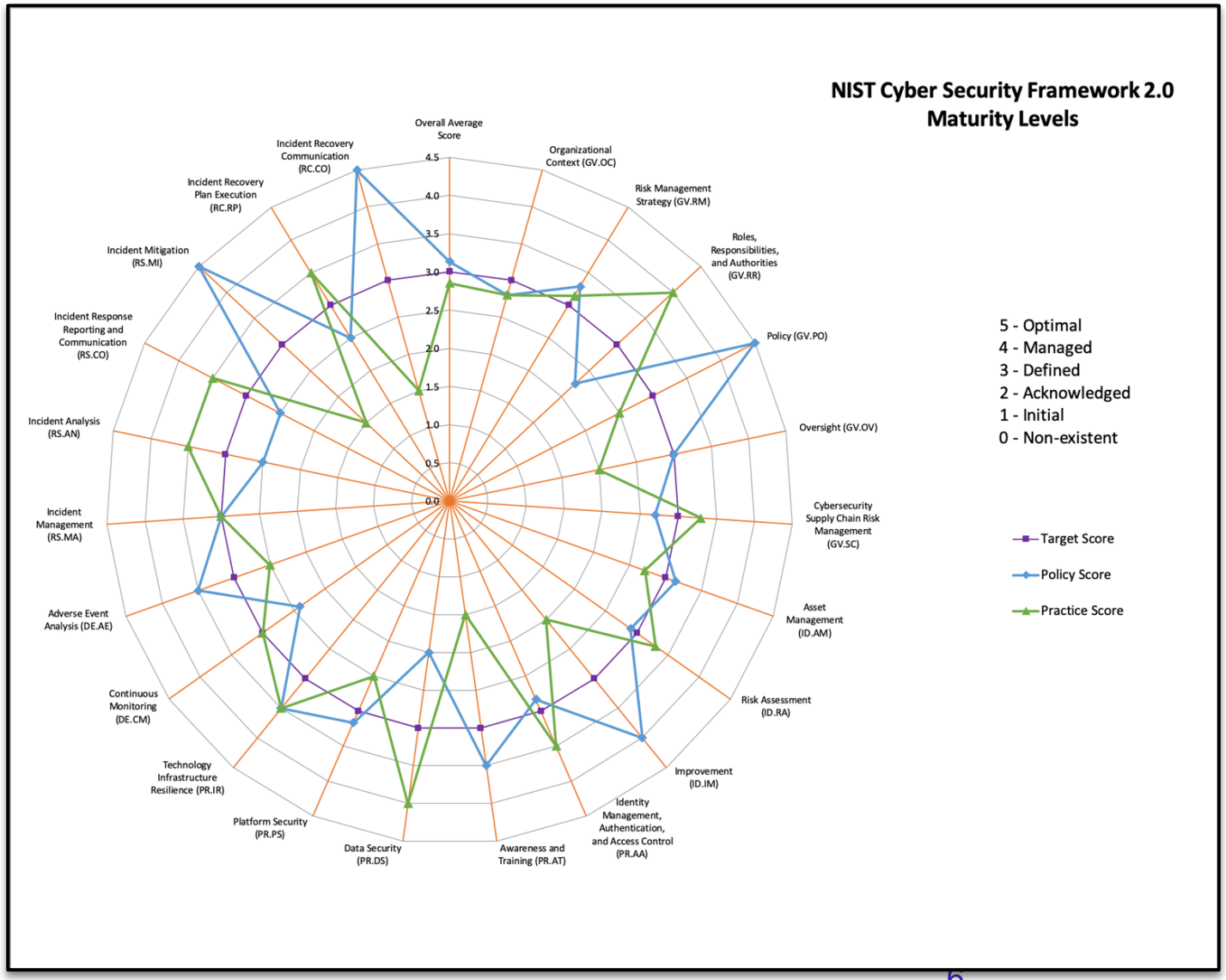
What the CSF is… And what it isn't



- The NIST CSF *is*:
  - Based on standards of good practice
  - A risk mitigation framework that is focused on uncovering risks
  - Open for implementation interpretation

- The NIST CSF *is not*:
  - A hard set series of mandates that you must* follow
  - A way to compare your company against other organizations
  - Required to be all-encompassing

History of the NIST CSF Maturity Toolkit



- Originally developed in 2015
- Released publicly in 2019 for CSF 1.1
- Updated to include the Privacy Framework 1.0 in 2020
- Updated to CSF 2.0 in 2024

SENTICON SECURITY
RSAC 2025 Conference

Why was the CMT built?

- Implementation tiers released in CSF 1.0 were NOT maturity levels
- CSF didn't line up with Enterprise IT maturity, so measurement was difficult
- The complexity of tier interpretation made things worse
- Had to address vague interpretation of compliance (Policy? Practice?)

Tier #	Description	Synopsis
Tier 1	Partial	Organizations at this tier have an ad hoc and reactive approach to managing cybersecurity risk with limited formal processes in place.
Tier 2	Risk Informed	Organizations at this level have begun to recognize and address cybersecurity risks in a more deliberate manner, though practices are not yet standardized across the entire organization.
Tier 3	Repeatable	Organizations at this level have established documented and repeatable cybersecurity processes that are consistently applied across the organization.
Tier 4	Adaptive	Organizations at this level proactively adapt their cybersecurity practices based on continuous monitoring, feedback, and real-time threat intelligence.

Why ‘Policy’ vs ‘Practice’?

Corporate Policy #1

All users MUST use strong, multi factor authentication when accessing internal corporate resources.

Practice: **The executive team doesn't want the ‘headache’ of using MFA and the AS/400 that processes million in revenue every month doesn't support it.**

Corporate Policy #2

Any vulnerability rated ‘critical’ must be patched within 72 hours of patch release.

Practice: **The production environment has scheduled quarterly outages when all pending patches are deployed**

Policy Maturity vs Practice Maturity

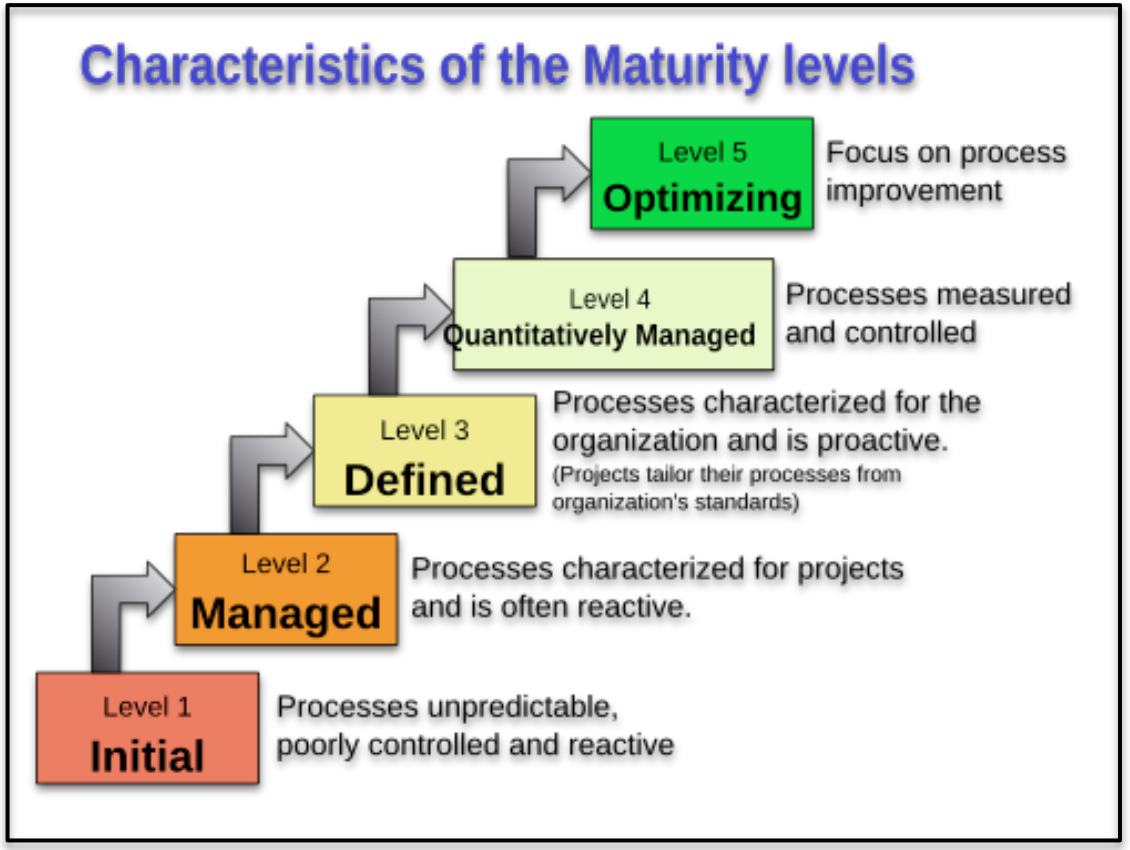
	NIST CSF 2.0 Categories	# Controls	Target Score	Policy Score	Practice Score
	Overall Average Score		3.00	3.14	2.85
GOVERN (GV)	Organizational Context (GV.OC)	(5)	3.00	2.80	2.80
	Risk Management Strategy (GV.RM)	(7)	3.00	3.29	3.14
	Roles, Responsibilities, and Authorities (GV.RR)	(4)	3.00	2.25	4.00
	Policy (GV.PO)	(2)	3.00	4.50	2.50
	Oversight (GV.OV)	(3)	3.00	3.00	2.00
	Cybersecurity Supply Chain Risk Management (GV.SC)	(10)	3.00	2.70	3.30
IDENTIFY (ID)	Asset Management (ID.AM)	(7)	3.00	3.14	2.71
	Risk Assessment (ID.RA)	(10)	3.00	2.90	3.30
	Improvement (ID.IM)	(4)	3.00	4.00	2.00
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)	(6)	3.00	2.83	3.50
	Awareness and Training (PR.AT)	(2)	3.00	3.50	1.50
	Data Security (PR.DS)	(4)	3.00	2.00	4.00
	Platform Security (PR.PS)	(6)	3.00	3.17	2.50
	Technology Infrastructure Resilience (PR.IR)	(4)	3.00	3.50	3.50
DETECT (DE)	Continuous Monitoring (DE.CM)	(5)	3.00	2.40	3.00
	Adverse Event Analysis (DE.AE)	(6)	3.00	3.50	2.50
RESPOND (RS)	Incident Management (RS.MA)	(5)	3.00	3.00	3.00
	Incident Analysis (RS.AN)	(4)	3.00	2.50	3.50
	Incident Response Reporting and Communication (RS.CO)	(2)	3.00	2.50	3.50
	Incident Mitigation (RS.MI)	(2)	3.00	4.50	1.50
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)	(6)	3.00	2.50	3.50
	Incident Recovery Communication (RC.CO)	(2)	3.00	4.50	1.50

- Too often, policies do not keep pace with technology
- Operational imperatives or business initiatives typically drive daily practices
- People tend to answer CSF questions based on policies because it's what they are 'supposed to do'
- Now, we can uncover the risk between policy and practice

SENTICON SECURITY

Five Levels of SEI-CMM Maturity

- Developed by Carnegie Mellon Software Engineering Institute (SEI) in the 1980s
- Capability Maturity Model defines 5 distinct maturity levels
- Use by organizations worldwide as a baseline measurement
- Aligns well with existing IT metrics and KPIs



SENTICON SECURITY
RSAC 2025 Conference

The Objective of the CMT

The Goal Of The Toolkit is..

To develop a holistic risk measurement tool that identified gaps in functional practice as well as documented policy.

RSAC | 2025 Conference

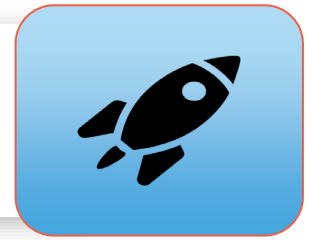
Customizing The Maturity Toolkit

Defining Maturity Levels

01

Purposeful

The maturity levels should set clear and supported direction for the entire organization



02

Actionable

The maturity levels should be realistic and achievable without unrealistic time frames or expectations.

03

Trackable

The maturity levels should be easily measurable and align with existing ITSM metrics and KPIs.

04

Continuous

The maturity levels should measured and reported on consistently.

Defining Policy Maturity Levels

Policy and standard exists with management approval. Less than .5% exceptions and they are documented.

Level 5 Optimizing

Level 4 Managed

Policy and standards exist with management approval. Less than 3% exceptions and are documented.

Policy and standard exists with management approval. Policy exceptions are documented & occur less than 5% of the time.

Level 3 Defined

Level 2 Repeatable

Policy or standard exists, but has not been reviewed in more than 2 years.

Policy or standard does not exist or is not formally approved by management.

Level 1 Initial

SENTICON SECURITY

RSAC 2025 Conference

Defining Process Maturity Levels

Formal process exists. Evidence & metrics collected for all activities. Less than 1% exceptions and are documented.

Level 5
Optimizing

Level 4
Managed

Formal process exists. Evidence & metrics collected all activities. Less than 5% exceptions occur.

Formal process exists and is documented. Evidence collected for most activities. Less than 10% exceptions.

Level 3
Defined

Level 2
Repeatable

Ad-hoc process exists and is done informally, with no metrics or KPIs

Standard, formal process does not exist.

Level 1
Initial

Sample Maturity Levels

Maturity Level	Expectation of Policy Maturity	Expectation of Process Maturity
Level 1 - Initial	Policy or standard does not exist or is not formally approved by management.	Standard process does not exist.
Level 2 - Repeatable	Policy or standard exists, but has not been reviewed in more than 2 years	Ad-hoc process exists and is done informally.
Level 3 - Defined	Policy and standard exists with formal management approval. Policy exceptions are documented, approved and occur less than 5% of the time.	Formal process exists and is documented. Evidence can be provided for most activities. Less than 10% exceptions.
Level 4 - Managed	Policy and standard exists with formal management approval. Policy exceptions are documented, approved and occur less than 3% of the time.	Formal process exists and is documented. Evidence can be provided for all activities and detailed metrics of the process are captured and reported. Minimal target for metrics has been established. Less than 5% of process exceptions occur with minimal recurring exceptions.
Level 5 - Optimizing	Policy and standard exists with formal management approval. Policy exceptions are documented, approved and occur less than 0.5% of the time.	Formal process exists and is documented. Evidence can be provided for all activities and detailed metrics of the process are captured and reported. Minimal target for metrics has been established and continually improving. Less than 1% of process exceptions occur.

Defining Target Maturity Score

	NIST CSF 2.0 Categories	# Controls	Target Score	Policy Score	Practice Score
	Overall Average Score		3.00	3.14	2.85
GOVERN (GV)	Organizational Context (GV.OC)	(5)	3.00	2.80	2.80
	Risk Management Strategy (GV.RM)	(7)	3.00	3.29	3.14
	Roles, Responsibilities, and Authorities (GV.RR)	(4)	3.00	2.25	4.00
	Policy (GV.PO)	(2)	3.00	4.50	2.50
	Oversight (GV.OV)	(3)	3.00	3.00	2.00
	Cybersecurity Supply Chain Risk Management (GV.SC)	(10)	3.00	2.70	3.30
IDENTIFY (ID)	Asset Management (ID.AM)	(7)	3.00	3.14	2.71
	Risk Assessment (ID.RA)	(10)	3.00	2.90	3.30
	Improvement (ID.IM)	(4)	3.00	4.00	2.00
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)	(6)	3.00	2.83	3.50
	Awareness and Training (PR.AT)	(2)	3.00	3.50	1.50
	Data Security (PR.DS)	(4)	3.00	2.00	4.00
	Platform Security (PR.PS)	(6)	3.00	3.17	2.50
	Technology Infrastructure Resilience (PR.IR)	(4)	3.00	3.50	3.50
DETECT (DE)	Continuous Monitoring (DE.CM)	(5)	3.00	2.40	3.00
	Adverse Event Analysis (DE.AE)	(6)	3.00	3.50	2.50
RESPOND (RS)	Incident Management (RS.MA)	(5)	3.00	3.00	3.00
	Incident Analysis (RS.AN)	(4)	3.00	2.50	3.50
	Incident Response Reporting and Communication (RS.CO)	(2)	3.00	2.50	3.50
	Incident Mitigation (RS.MI)	(2)	3.00	4.50	1.50
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)	(6)	3.00	2.50	3.50
	Incident Recovery Communication (RC.CO)	(2)	3.00	4.50	1.50

- Target Score is the agreed to maturity level for the assessment.
- Based on Maturity Levels previously defined.
- Since Policy and Practice should be at the same maturity, there is only one Target Score for each sub-category.

RSAC | 2025 Conference

Performing the Assessment

Example #1 PR.AA-01

IDENTIFY (ID)
PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

Category	Subcategory	Implementation Examples	Informative References
Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access			**CRI Profile v2.0: PR.AA** **CSF v1.1: PR.AC**

Subcategory	Implementation Examples	Informative References	Policy Maturity	Policy Score Reasoning	Practice Maturity	Practice Score Reasoning
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	**1st**: 1st Party Risk **Ex1**: Initiate requests for new access or additional access for employees, contractors, and others, and track, review, and fulfill the requests, with permission from system or data owners when needed **Ex2**: Issue, manage, and revoke cryptographic certificates and identity tokens, cryptographic keys (i.e., key management), and other credentials **Ex3**: Select a unique identifier for each device from immutable hardware characteristics or an identifier securely provisioned to the device **Ex4**: Physically label authorized hardware with an identifier for inventory and servicing purposes	**CIS Controls v8.0: 5.1** **CIS Controls v8.0: 6.7** **CRI Profile v2.0: PR.AA-01** **CRI Profile v2.0: PR.AA-01.01** **CRI Profile v2.0: PR.AA-01.02** **CSF v1.1: PR.AC-1**	2.0	Policy or standard exists, but has not been reviewed in more than 2 years.	3.0	Formal process exists and is documented. Evidence collected for most activities. Less than 10% exceptions.

Example #2 PR.PS-01

IDENTIFY (ID)

PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

Category	Subcategory	Implementation Examples	Informative References
Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability			**CRI Profile v2.0: PR.PS**

Subcategory	Implementation Examples	Informative References	Policy Maturity	Policy Score Reasoning	Practice Maturity	Practice Score Reasoning
PR.PS-01: Configuration management practices are established and applied	**1st**: 1st Party Risk **Ex1**: Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality) **Ex2**: Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software **Ex3**: Monitor implemented software for deviations from approved baselines	**SP 800-218: PO.5.2** **SP 800-218: PS.1.1** **CIS Controls v8.0: 4.1** **CIS Controls v8.0: 4.2** **CRI Profile v2.0: PR.PS-01** **CRI Profile v2.0: PR.PS-01.01** **CRI Profile v2.0: PR.PS-01.02** **CRI Profile v2.0: PR.PS-01.03** **CRI Profile v2.0: PR.PS-01.04** **CRI Profile v2.0: PR.PS-01.05** **CRI Profile v2.0: PR.PS-01.06** **CRI Profile v2.0: PR.PS-01.07** **CRI Profile v2.0: PR.PS-01.08** **CRI Profile v2.0: PR.PS-01.09** **CSF v1.1: PR.IP-1** **CSF v1.1: PR.IP-3** **CSF v1.1: PR.PT-2** **CSF v1.1: PR.PT-3**	4.0	Policy and standards exist with management approval. Less than 3% exceptions and are documented	3.0	Formal process exists and is documented. Evidence collected for most activities. Less than 10% exceptions.

Example #3 DE.CM-01

PROTECT (PR)
DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed

Category	Subcategory	Implementation Examples	Informative References
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events			**CRI Profile v2.0: DE.CM** **CSF v1.1: DE.CM**

Subcategory	Implementation Examples	Informative References	Policy Maturity	Policy Score Reasoning	Practice Maturity	Practice Score Reasoning
DE.CM-01: Networks and network services are monitored to find potentially adverse events	**Ex1**: Monitor DNS, BGP, and other network services for adverse events **Ex2**: Monitor wired and wireless networks for connections from unauthorized endpoints **Ex3**: Monitor facilities for unauthorized or rogue wireless networks **Ex4**: Compare actual network flows against baselines to detect deviations **Ex5**: Monitor network communications to identify changes in security postures for zero trust purposes **1st**: 1st Party Risk	**CIS Controls v8.0: 13.1** **CRI Profile v2.0: DE.CM-01** **CRI Profile v2.0: DE.CM-01.01** **CRI Profile v2.0: DE.CM-01.02** **CRI Profile v2.0: DE.CM-01.03** **CRI Profile v2.0: DE.CM-01.04** **CRI Profile v2.0: DE.CM-01.05** **CRI Profile v2.0: DE.CM-01.06** **CSF v1.1: DE.CM-1** **CSF v1.1: DE.CM-4** **CSF v1.1: DE.CM-5** **CSF v1.1: DE.CM-7**	4.0	Policy and standards exist with management approval. Less than 3% exceptions and are documented	1.0	Standard, formal process does not exist.

Example #4 DE.CM-05

PROTECT (PR)
DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed

Category	Subcategory	Implementation Examples	Informative References
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events			**CRI Profile v2.0: DE.CM** **CSF v1.1: DE.CM**

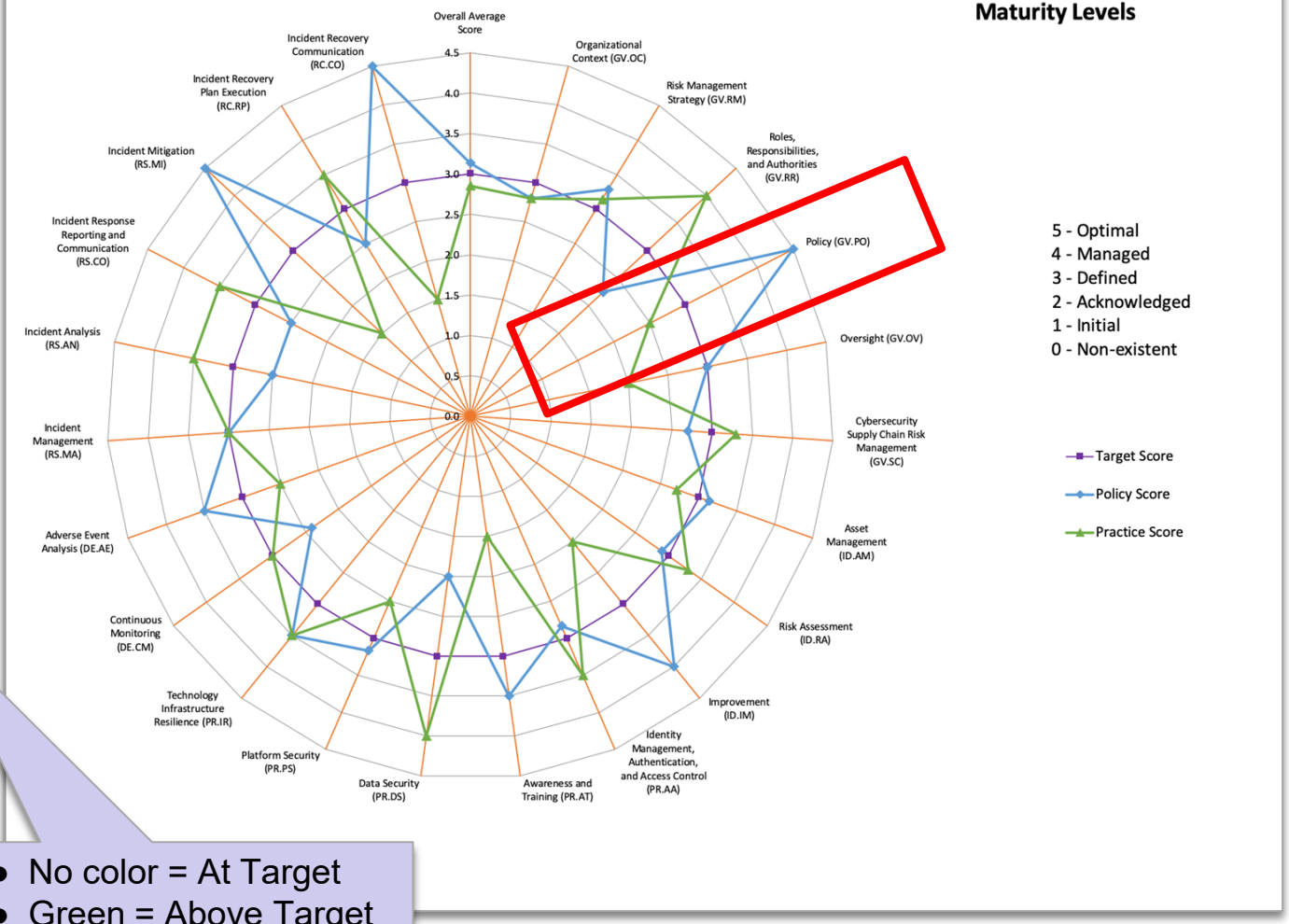
Subcategory	Implementation Examples	Informative References	Policy Maturity	Policy Score Reasoning	Practice Maturity	Practice Score Reasoning
DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	**Ex1**: Monitor email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks and exfiltration, and other adverse events **Ex2**: Monitor authentication attempts to identify attacks against credentials and unauthorized credential reuse **Ex3**: Monitor software configurations for deviations from security baselines **Ex4**: Monitor hardware and software for signs of tampering **Ex5**: Use technologies with a presence on endpoints to detect cyber health issues (e.g., missing patches, malware infections, unauthorized software), and redirect the endpoints to a remediation environment before access is authorized **1st**: 1st Party Risk	**CIS Controls v8.0: 10.1** **CRI Profile v2.0: DE.CM-09** **CRI Profile v2.0: DE.CM-09.01** **CRI Profile v2.0: DE.CM-09.02** **CRI Profile v2.0: DE.CM-09.03** **CSF v1.1: PR.DS-6** **CSF v1.1: PR.DS-8** **CSF v1.1: DE.CM-4** **CSF v1.1: DE.CM-5** **CSF v1.1: DE.CM-7**	2.0	Policy or standard exists, but has not been reviewed in more than 2 years.	5.0	Formal process exists. Evidence & metrics collected for all activities. Less than 1% exceptions and are documented.

SENTICON SECURITY
RSAC 2025 Conference

Reviewing the Results

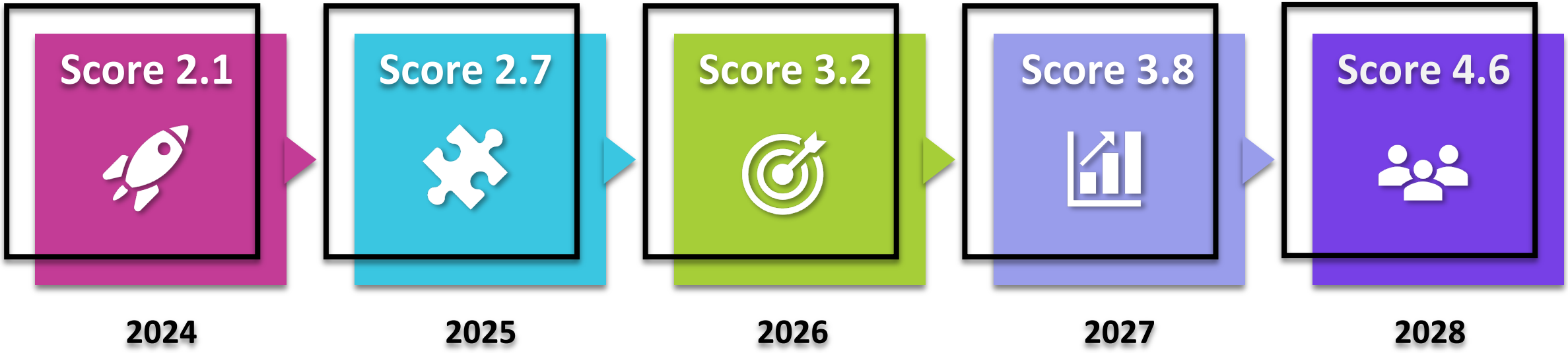
The overall average score for the assessment

	NIST CSF 2.0 Categories	# Controls	Target Score	Policy Score	Practice Score
	Overall Average Score		3.00	3.14	2.85
GOVERN (GV)	Organizational Context (GV.OC)	(5)	3.00	2.80	2.80
	Risk Management Strategy (GV.RM)	(7)	3.00	3.29	3.14
	Roles, Responsibilities, and Authorities (GV.RR)	(4)	3.00	2.25	4.00
	Policy (GV.PO)	(2)	3.00	4.50	2.50
	Oversight (GV.OV)	(3)	3.00	3.00	2.00
	Cybersecurity Supply Chain Risk Management (GV.SC)	(10)	3.00	2.70	3.30
IDENTIFY (ID)	Asset Management (ID.AM)	(7)	3.00	3.14	2.71
	Risk Assessment (ID.RA)	(10)	3.00	2.90	3.30
	Improvement (ID.IM)	(4)	3.00	4.00	2.00
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)	(6)	3.00	2.83	3.50
	Awareness and Training (PR.AT)	(2)	3.00	3.50	1.50
	Data Security (PR.DS)	(4)	3.00	2.00	4.00
	Platform Security (PR.PS)	(6)	3.00	3.17	2.50
	Technology Infrastructure Resilience (PR.IR)	(4)	3.00	3.50	3.50
DETECT (DE)	Continuous Monitoring (DE.CM)	(5	3.00	2.40	3.00
	Adverse Event Analysis (DE.AE)	(6	3.00	3.50	2.50
RESPOND (RS)	Incident Management (RS.MA)	(5)	3.00	3.00	3.00
	Incident Analysis (RS.AN)	(4)	3.00	2.50	3.50
	Incident Response Reporting and Communication (RS.CO)	(2)	3.00	2.50	3.50
	Incident Mitigation (RS.MI)	(2)	3.00	4.50	1.50
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)	(6)	3.00	2.50	3.50
	Incident Recovery Communication (RC.CO)	(2)	3.00	4.50	1.50



- No color = At Target
- Green = Above Target
- Red = Under Target

It's Not 'One & Done'



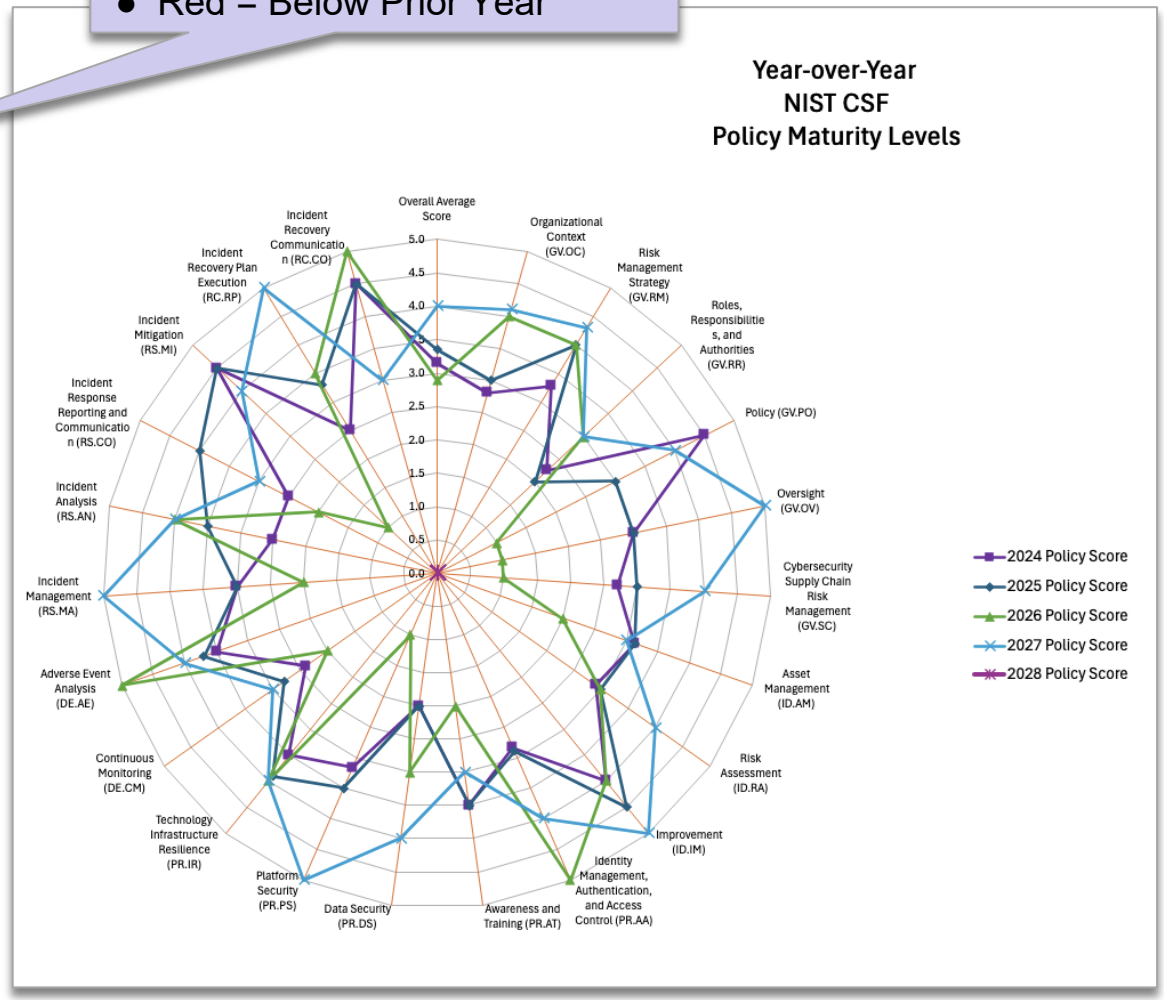
Demonstrating Maturation

The power of the Toolkit is enabling an 'Apples to Apples' comparison of security maturity over multiple years ***or*** after major security initiatives.

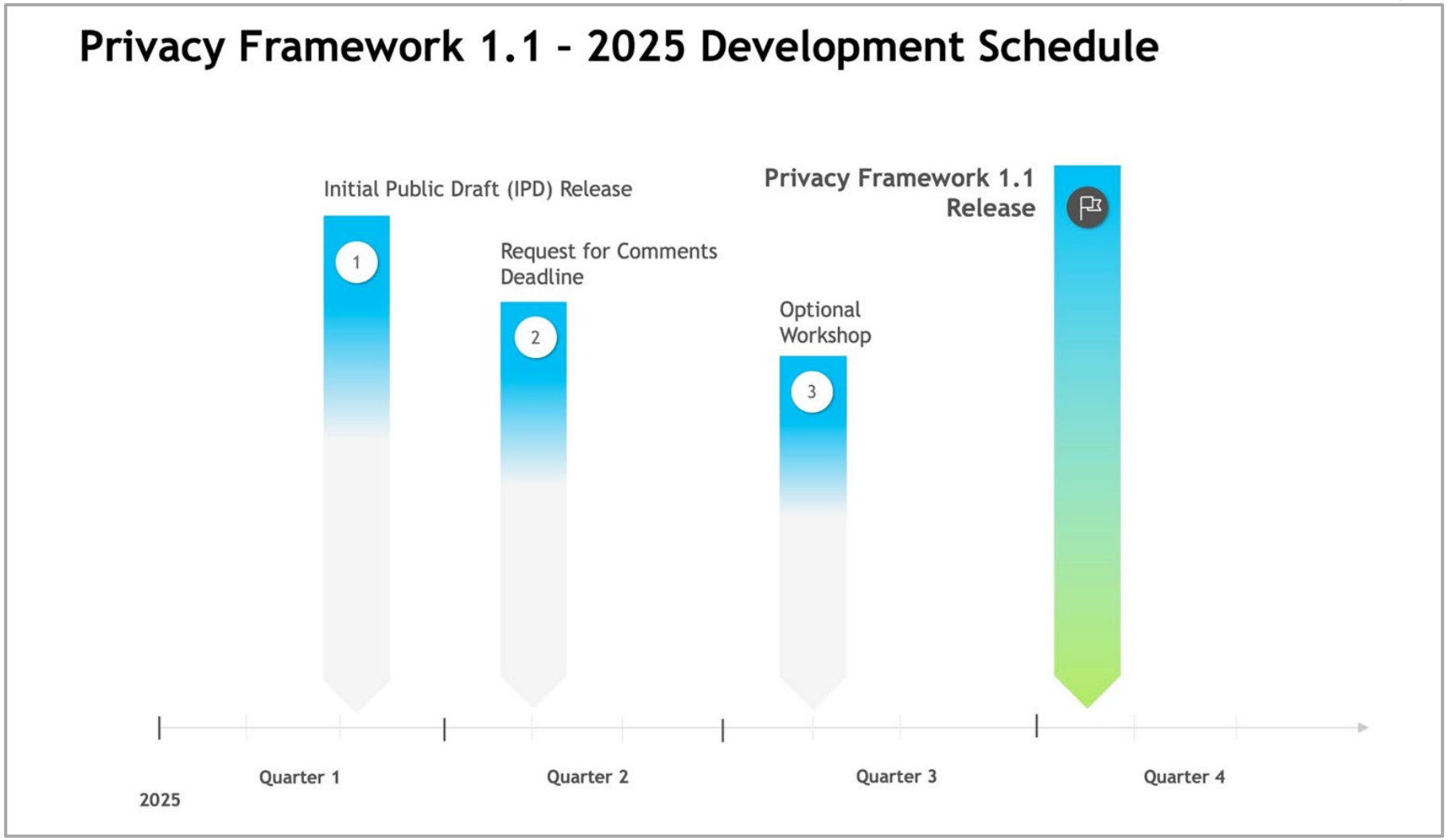
Year Over Year Reporting

- No color = No Change
- Green = Above Prior Year
- Red = Below Prior Year

	NIST CSF 2.0 Categories - Policy	# Controls	Target Score	2024 Policy Score	2025 Policy Score	2026 Policy Score	2027 Policy Score	2028 Policy Score
	Overall Average Score		3.00	3.14	3.35	2.89	4.00	0.00
GOVERN (GV)	Organizational Context (GV.OC)	(5)	3.00	2.80	3.00	4.00	4.10	0.00
	Risk Management Strategy (GV.RM)	(7)	3.00	3.29	4.00	4.00	4.30	0.00
	Roles, Responsibilities, and Authorities (GV.RR)	(4)	3.00	2.25	2.00	3.00	3.00	0.00
	Policy (GV.PO)	(2)	3.00	4.50	3.00	1.00	4.00	0.00
	Oversight (GV.OV)	(3)	3.00	3.00	3.00	1.00	5.00	0.00
	Cybersecurity Supply Chain Risk Management (GV.SC)	(10)	3.00	2.70	3.00	1.00	4.00	0.00
IDENTIFY (ID)	Asset Management (ID.AM)	(7)	3.00	3.14	3.14	2.00	3.00	0.00
	Risk Assessment (ID.RA)	(10)	3.00	2.90	3.00	3.00	4.00	0.00
	Improvement (ID.IM)	(4)	3.00	4.00	4.50	4.00	5.00	0.00
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR..	(6)	3.00	2.83	2.90	5.00	4.00	0.00
	Awareness and Training (PR.AT)	(2)	3.00	3.50	3.50	2.00	3.00	0.00
	Data Security (PR.DS)	(4)	3.00	2.00	2.00	3.00	4.00	0.00
	Platform Security (PR.PS)	(6)	3.00	3.17	3.50	1.00	5.00	0.00
	Technology Infrastructure Resilience (PR.IR)	(4)	3.00	3.50	3.90	4.00	4.00	0.00
DETECT (DE)	Continuous Monitoring (DE.CM)	(5)	3.00	2.40	2.80	2.00	3.00	0.00
	Adverse Event Analysis (DE.AE)	(6)	3.00	3.50	3.70	5.00	4.00	0.00
RESPOND (RS)	Incident Management (RS.MA)	(5)	3.00	3.00	3.00	2.00	5.00	0.00
	Incident Analysis (RS.AN)	(4)	3.00	2.50	3.50	4.00	4.00	0.00
	Incident Response Reporting and Communication (RS.CO)	(2)	3.00	2.50	4.00	2.00	3.00	0.00
	Incident Mitigation (RS.MI)	(2)	3.00	4.50	4.50	1.00	4.00	0.00
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)	(6)	3.00	2.50	3.30	3.50	5.00	0.00
	Incident Recovery Communication (RC.CO)	(2)	3.00	4.50	4.50	5.00	3.00	0.00



Privacy Framework 1.1 - Coming 2025



RSAC | 2025 Conference

Live Demo

Apply What You Have Learned Today

- Next week you should:
  - Download the latest version from GitHub
  - Identify a business line or internal group for an assessment
- In the first month following this presentation you should:
  - Define the Target Goals for each category and the ‘Maturity Levels’
  - Perform initial limited assessment on selected organization
- Within six months you should:
  - Have identified key ‘high risk’ situations within the enterprise
  - Developed strategic plans to mitigate risk and raise mature score

RSAC | 2025 Conference

Many Voices. One Community.

Thank You!

Any questions?

(E) John.Masserini@SentiCon-Security.com

(W) SentiCon-Security.com

LinkedIn: linkedin.com/in/jjmasserini/

Repo: github.com/SentiConSecurity/NIST_CSF_Maturity_Tool

GitHub Repo

LinkedIn Profile